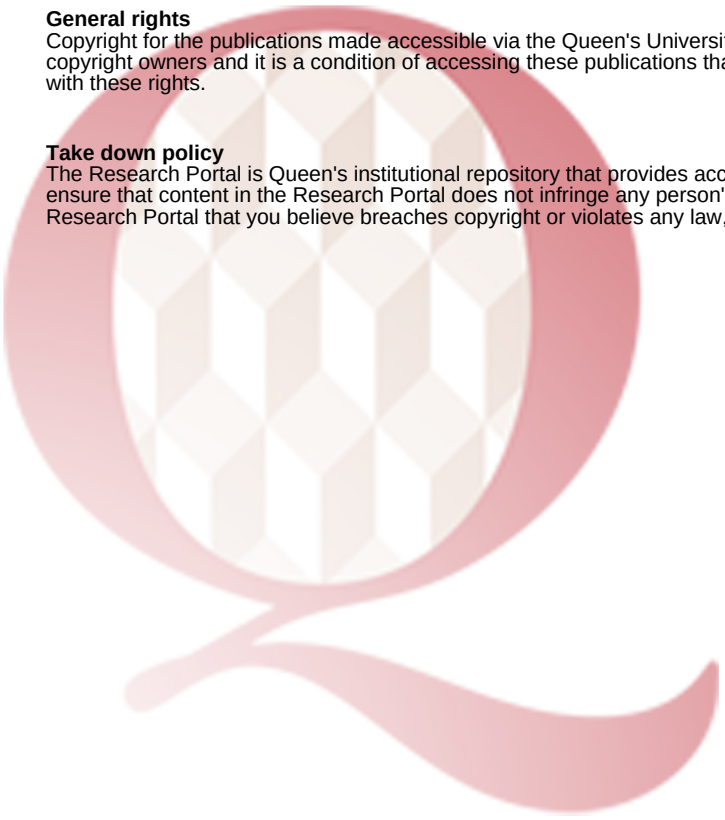
# Signal Reception Characteristics in the Proximity of Alice and Bob for Secure Indoor Peer-to-Peer Communications At 2.45 GHz





# Signal Reception Characteristics in the Proximity of Alice and Bob for Secure Indoor Peer-to-Peer Communications At 2.45 GHz

# Signal Reception Characteristics in the Proximity of Alice and Bob for Secure Indoor Peer-to-Peer Communications at 2.45 GHz

Nidhi Bhargav, Simon L. Cotton and Vincent F. Fusco
Institute of Electronics, Communication & Information Technology
Queen's University Belfast, BT3 9DT, UK
{nbhargav01, simon.cotton, v.fusco}@qub.ac.uk

***Abstract*—Mutual variation of the received signal which occurs as a consequence of the channel reciprocity property has recently been proposed as a viable method for secret key generation. However, this cannot be strictly maintained in practice as the property is applicable only in the absence of interference. To ensure the propagation defined key remains secret, one requirement is that there remain high degrees of uncertainty between the legitimate users channel response and that of any eavesdropper's. In this paper, we investigate whether such de-correlation occurs for an indoor point-to-point link at 2.45 GHz. This is achieved by computing the *localized* correlation coefficient between the simultaneous channel response measured by the legitimate users and that of multiple distributed eavesdroppers for static and dynamic scenarios.**

***Index Terms*—secure communication, physical layer security, measurements, correlation, fading characteristics, indoor communication.**

## I. INTRODUCTION

Privacy and security in wireless communication networks is a fundamental requirement. The inherent broadcast nature of the wireless medium poses different challenges in achieving secure communications in the presence of unintended recipients. Up until now, secure communication relied on classical cryptographic techniques, e.g., the Diffie-Hellman key exchange protocol [1]. The problem with these techniques is that they are computationally expensive, consume significant amounts of power and do not achieve information theoretic security. Shannon [2] defined this as occurring when the entropy $H(M|C) = H(M)$; where $M$ is the plain text message and $C$ is its corresponding encryption. Recently, there has been a significant amount of research into physical layer security techniques that take advantage of the inherent channel randomness to generate secret keys [3]. The advantage of such techniques is that they are, in theory, capable of achieving information theoretic secrecy.

Additionally there has also been work [4-8] on exploiting the multipath characteristics of the wireless channel to estimate the received signal strength for extracting the secret information bits shared between legitimate parties. The channel's phase has also been explored for secret key generation in [9, 10]. What is common amongst these studies is that they all rely on the unpredictability of the channel state when considering the channel as a source of randomness for key generation. Under the assumption that an eavesdropper's channel is uncorrelated with the channel between the legitimate parties, the eavesdropper is unable to establish the secret key.

While key generation can be achieved from the statistical nature of the channel; to ensure secrecy, it is important that any eavesdropping channel remain sufficiently de-correlated with that of the legitimate users. It is therefore necessary to understand when such de-correlation occurs. In this paper, we investigate experimentally whether the characteristics of the received signal at potential eavesdropping positions are suitably uncorrelated with the signal characteristics at the legitimate parties. This is done by calculating the correlation coefficient of the received signal envelope at the legitimate users' (designated as Alice and Bob) and multiple eavesdroppers (Eve's) distributed throughout the local surroundings. Our analysis takes place within an indoor environment at 2.45 GHz.

This paper is organized as follows. Section II describes the experimental setup and the measurement procedure. Section III contains a comparison of received signal power time series and correlation coefficient results between Alice, Bob and Eves for a static scenario and then a dynamic scenario in an indoor environment. Lastly, Section IV presents some concluding remarks and also suggests some future directions for the work.

## II. EXPERIMENTAL SETUP AND MEASUREMENTS

The measurements conducted in this study were carried out for a point-to-point link in an open office environment located on the first floor of the ECIT building at Queen's University Belfast in the United Kingdom. The building mainly consists of metal studded dry walls with metal tiled floors covered with polypropylene-fiber, rubber backed carpet tiles, a metal ceiling with mineral fiber tiles and recessed louvered luminaries suspended 2.7 m above floor level.

This work was supported by the Department of Education and Learning (DEL) NI and in part by the U.K. Royal Academy of Engineering and the Engineering and Physical Research Council (EPSRC) under Grant Reference EP/H044191/1 and EP/L026074/1, and also by the Leverhulme Trust, UK.

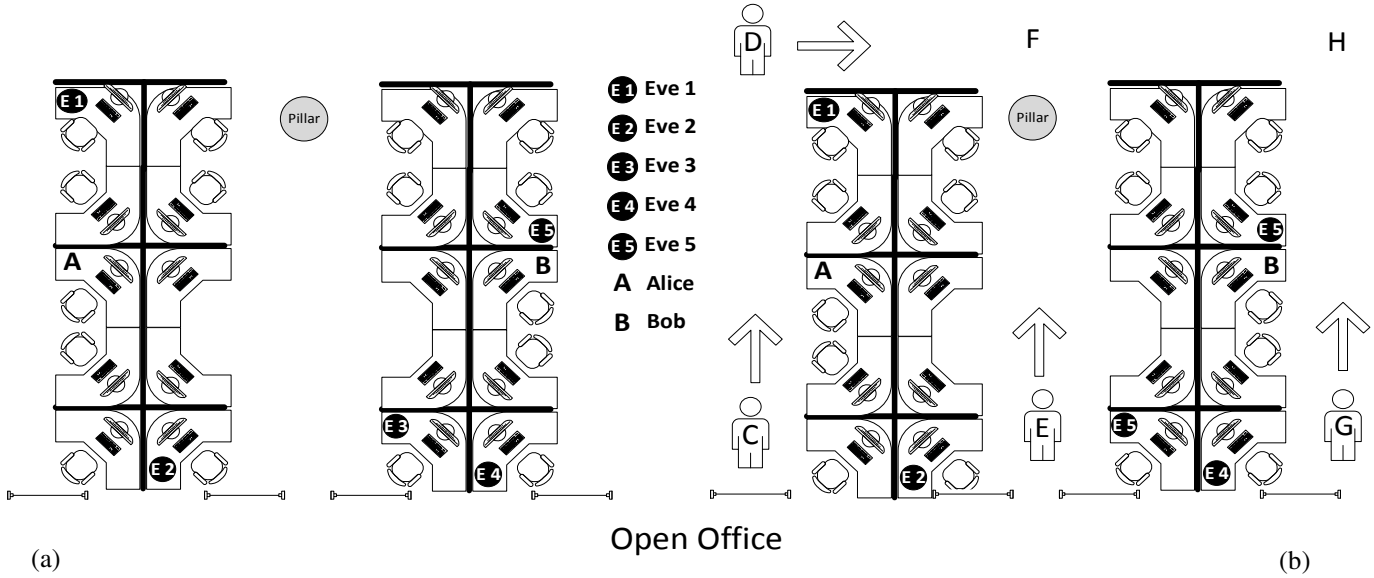



Fig.1 Open office area showing the position of Alice (node A), Bob (node B) and multiple Eves (node E's) for (a) static scenario and (b) dynamic scenario. Four pedestrians walked simultaneously from point C to point D, point D to point H, point E to point F and point G to point H, respectively for the dynamic scenario and the office was left unoccupied for the static scenario.

The office contained a number of chairs, metal storage spaces, doors and desks constructed from medium density fiberboard. These desks were vertically separated by soft wooden partitions.

As illustrated in Fig. 1, two different scenarios were considered. These were: (1) static scenario [Fig. 1(a)] and (2) dynamic scenario [Fig. 1(b)]. The desired point-to-point link was established between two legitimate parties, Alice (node A), and Bob (node B) whilst multiple co-located Eves (node E's) were attempting to eavesdrop. Each of the Alice, Bob and Eve nodes consisted of an ML2730 transceiver, manufactured by RFMD. The transceiver boards were interfaced with a PIC32MX microcontroller which acted as a baseband controller and allowed the analog received signal strength indicator (RSSI) to be sampled with a 10-bit quantization depth. For the channel measurements conducted here, Alice acted as the transmitter outputting a continuous wave signal with a power of +21 dBm.

Alice transmitted first by sending a trigger pulse to all the radio receivers. The receivers started the signal capture when they received the trigger signal for a duration of 10 seconds. These measurements were then repeated with Bob acting as the transmitter and Alice being the receiver. All the other nodes were configured to record the RSSI simultaneously (i.e. time synchronized) with a sample frequency of 1 kHz. They utilized identical sleeve dipole antennas (Mobile Mark model PSKN3-24/555) which featured an omnidirectional radiation pattern in the azimuth and elevation. They were vertically polarized throughout all of the experiments.

The experiments were performed in a choreographed manner when the office was unoccupied except for the four test subjects who moved in a repeatable manner for the experiments requiring motion. It should be noted that in order to enable as realistic a characterization of the signal correlation as possible, the wireless spectrum at the measurement frequency was uncontrolled, that is other wireless devices operating within the test environment may have acted as sources of interference.

In this study we considered two typical peer-to-peer scenarios. Our first experiment, herein referred to as *experiment 1*, was performed for a static scenario [Fig. 1(a)], wherein the office was left unoccupied for the entire duration of the measurements. Please note that people still remained in other floors of the building and their movement was uncontrolled. The second experiment, herein referred to as *experiment 2*, was performed when the office was unoccupied except for four pedestrians who moved simultaneously from point C to point D, point D to point H, point E to point F and point G to point H, respectively [Fig. 1(b)].

## III. Results and Analysis

### A. Static Scenario (Experiment 1)

This experiment was conducted to study the channel variations observed for a quasi-stationary scenario. The correlation coefficient between Alice- Bob, Alice-Eve and Bob-Eve channels were computed for a moving window of 0.5 seconds over a 10 second period. This computation was based on the Pearson product-moment correlation coefficient:

$$r = \frac{\sum_{i=1}^{n}(X_i - \overline{X})(Y_i - \overline{Y})}{\sqrt{\sum_{i=1}^{n}(X_i - \overline{X})^2}\sqrt{\sum_{i=1}^{n}(Y_i - \overline{Y})^2}} \qquad (1)$$

where, $X_i$ and $Y_i$ are the RSSI values of the $i$th packet of each node. $\overline{X}$ and $\overline{Y}$ are the respective mean RSSI values of a sequence of $n$ packets. Also, it should be noted that the

correlation coefficient was calculated using the *linear amplitude* of the signal.

Table I presents the mean and standard deviation of the correlation coefficients for this scenario. As we can see the mean correlation coefficients obtained here between the Alice-Bob, Alice-Eve and Bob-Eve channels were generally quite low. Although channel reciprocity was observed for the static scenario, a high de-correlation between the legitimate users' is seen. As the mean signal level remains relatively constant for this case, the high de-correlation between the legitimate nodes is mainly due to fluctuations in the received signal caused by the receiver noise that are de-correlated.

The highest observed correlation coefficient over the duration of experiment 1 was found to be 0.88, which occurred for the Bob-Eve 5 channel. The localized correlation coefficient for the Alice-Bob link was found to be 0.34. As indicated previously, to ensure secure communication and hence secret key generation, it is necessary for the eavesdroppers' link to remain sufficiently de-correlated with that of the legitimate users'. Thus, the results for the static scenario indicate that it is not a suitable environment for secret key generation.

### *B. Dynamic Scenario (Experiment 2)*

Figs. 2 and 3 show the variation of the received signal power measured by Alice, Bob and Eves with Alice as the transmitter and then Bob as the transmitter. As an example of the short-term fading behavior, Figs. 2 and 3 also show an expanded 0.5 second excerpt of the recorded waveform. As we can see the pedestrian movement in the open office environment causes significant variations in the signal power received by Alice, Eve 1 and Eve 3.

Table I provides the mean and standard deviation of the localized correlation coefficient for experiment 2. Although the spread of the correlation coefficient increased slightly, overall it still appears to be quite low. However, the localized correlation coefficient observed for Alice-Bob channel is 0.63 that is higher than the localized correlation coefficients observed for all Alice-Eve and Bob-Eve channels. Fig. 4 shows the empirical probability densities of the correlation coefficients calculated by comparing the Alice-Bob channel with that of Alice-Eve 1 and Bob-Eve 1 channels, respectively. It can be seen that the highest correlation coefficient values for Bob-Eve1 and Alice-Eve1 are 0.58 and 0.56, respectively which is lower than the value observed at Alice-Bob channel. Thus, the eavesdroppers are sufficiently de-correlated with Alice and Bob. Based on these results, it appears that the potential for secure communications by propagation means for indoor point-to-point links at 2.45 GHz exists for a dynamic environment. This indicates that a mobile environment is suitable for generating secret keys.

TABLE I. MEAN AND STANDARD DEVIATIONS OF THE LOCALIZED CORRELATION COEFFICIENTS FOR EACH OF THE SCENARIOS

| **Eavesdroppers** | Eve 1 | | Eve 2 | | Eve 3 | | Eve 4 | | Eve 5 | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| **Legitimate Receivers** | Alice | Bob | Alice | Bob | Alice | Bob | Alice | Bob | Alice | Bob | Alice-Bob |
| **EXPERIMENT 1: STATIC SCENARIO** | | | | | | | | | | | |
| **Mean *(μ)*** | 0.20 | 0.30 | 0.35 | 0.26 | 0.03 | 0.04 | 0.09 | 0.02 | 0.63 | 0.64 | -0.02 |
| **Std. Deviation *(σ)*** | 0.19 | 0.24 | 0.19 | 0.28 | 0.12 | 0.22 | 0.10 | 0.26 | 0.07 | 0.18 | 0.10 |
| **EXPERIMENT 2: DYNAMIC SCENARIO** | | | | | | | | | | | |
| **Mean *(μ)*** | 0.10 | 0.12 | 0.10 | 0.07 | 0.09 | -0.00 | -0.04 | 0.09 | 0.09 | 0.31 | 0.03 |
| **Std. Deviation *(σ)*** | 0.22 | 0.17 | 0.19 | 0.21 | 0.20 | 0.19 | 0.16 | 0.28 | 0.06 | 0.21 | 0.17 |

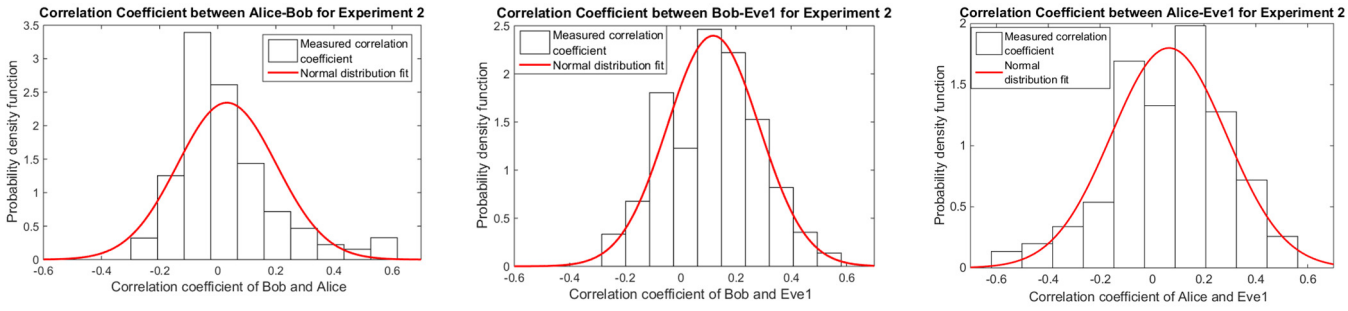



Fig.4 Correlation coefficients calculated between a) Alice-Bob b) Bob-Eve 1 and c) Alice-Eve1. Also shown for comparison is the theoretical Gaussian probability density function which is shown to provide an excellent fit to the data.

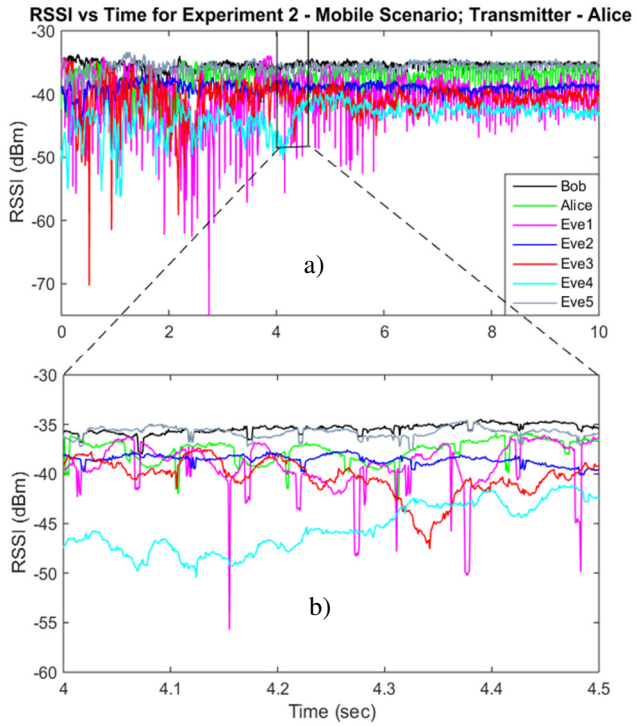



Fig. 2 RSSI (dBm) versus time (sec) for Experiment 2 – dynamic scenario with Alice as the transmitter; a) 10 seconds duration and below b) expanded section between 4 and 4.5 seconds.

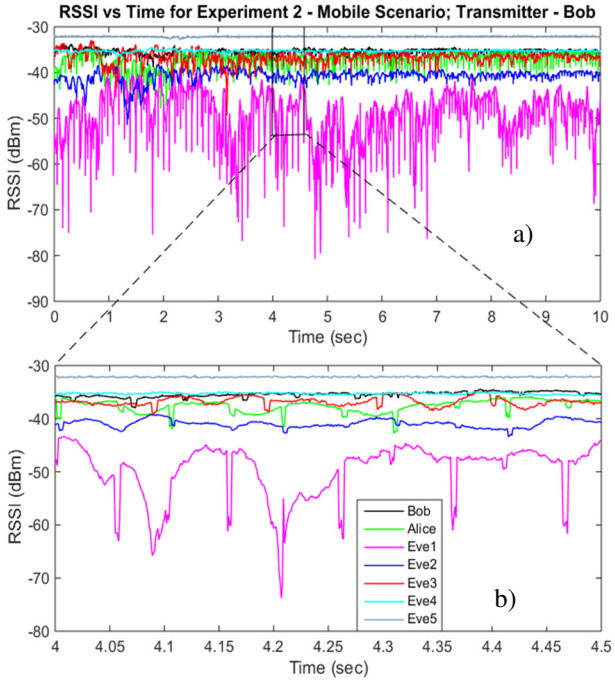



Fig. 3 RSSI (dBm) versus time (sec) for Experiment 2 –dynamic scenario with Bob as the transmitter; a) 10 seconds duration and below b) expanded section between 4 and 4.5 seconds.

## IV. Conclusion and Future Work

By measuring the signal received by multiple eavesdroppers in the vicinity of a legitimate indoor point-to-point link operating at 2.45 GHz, we have been able to calculate the localized correlation between the desired and the undesired links. The results suggest that it is possible to generate secret keys and hence achieve secure communications in a dynamic indoor environment. Future work will assess the mutual information between the legitimate users' and the eavesdroppers. We will also consider the impact of antenna type and polarization for this type of indoor peer-to-peer scenario.

## References


[1] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory,* vol. 22, no. 6, pp. 644-654, Nov 1976.

[2] C. E. Shannon, "Communication theory of secrecy systems," *Bell System Technical Journal*, vol. 28, no. 4, pp. 656-715, 1949.

[3] U. M. Maurer, "Secret key agreement by public discussion from common information," *IEEE Transactions on Information Theory*, vol. 39, no. 3, pp. 733-742, 1993.

[4] S. Mathur, W. Trappe, N. Mandayam, C. Ye, and A. Reznik, "Radio-telepathy: Extracting a secret key from an unauthenticated wireless channel," in *MobiCom'08*.

[5] B. Azimi-Sadjadi, A. Kiayias, A. Mercado, and B. Yener, "Robust key generation from signal envelopes in wireless networks," in *CCS'07*.

[6] M. A. Tope and J. C. McEachen, "Unconditionally secure communications over fading channels," *Proc. Military Comm. Conf. (MILCOM'01)*, vol. 1, pp. 54-58, Oct 2001.

[7] T. Aono, K. Higuchi, T. Ohira, B. Komiyama, and H. Sasaoka, "Wireless secret key generation exploiting reactance-domain scalar response of multipath fading channels," *IEEE Transactions on Antennas and Propagation*, vol. 53, no. 11, pp. 3776-3784, Nov 2005.

[8] S. Jana, S. N. Premnath, M. Clark, S. Kasera, N. Patwari, and S. V. Krishnamurthy, "On the effectiveness of secret key extraction from wireless signal strengths in real environments," in *Proc. ACM MobiCom*, Sep. 2009, pp. 321-332.

[9] A. Sayeed and A. Perrig, "Secure wireless communications: secret keys through multipath," *IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP '08)*, pp. 3013-3016, March 2008.

[10] Q. Wang, H. Su, K. Ren, and K. Kim, "Fast and scalable secret key generation exploiting channel phase randomness in wireless networks," *IEEE INFOCOM, 2011*, pp. 1422-1430, April 2011.